UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,772	07/21/2000	Raynold M. Kahn	PD-200045	3987

20991 7590 08/15/2006

THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/620,772	KAHN ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-29 and 31-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-29 and 31-50* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *21 April 2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 21 April 2006, with acknowledgement of an original application filed on 21 July 2000.

2. Claims 1, 2, 4-29, and 31-50 are pending, claims 1, 17, and 28 are independent claims.

3. The IDS submitted 21 April 2006 has been considered.

Claim Objections

4. Claims 1 and 28 are objected to because of the following informalities: the words 'releasably coupleable' are misspelled. Appropriate correction is required.

Specification

5. The disclosure is objected to because of the following informalities: the word 'coupleable' is misspelled. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1 and 28, as well as their dependent claims 2, 4-16, 43-46 and 29-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Examiner can find no reference in the specification for 'releasably coupleable' the closest explanation provided appears on page 11, lines 22-30, in which the IRD 132 is communicatively coupleable (spelling) to a conditional access module (CAM) 406.

Continued Examination Under 37 CFR 1.114

8. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 31 May 2005, fee has been entered. Examiner notes the search was updated due to the filing of the RCE; therefore prior art used in the below rejection was not publish at the time (18 January 2005) when this application was previous allowed.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 1, 2, 15, 17, 18, 25, 26, 27, 28, 29, 36, 40, 41, and 43,** are rejected under 35 U.S.C. 103(a) as being unpatentable over 'Okabe et al. US Patent No. 6,889,208 (hereinafter '208).

As to independent claim 1, "A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising

the steps of: (a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data" is taught in '208 col. 7, lines 13-25;

"(b) decrypting the received access control information in a conditional access module releaseably coupleable with the receive to produce the first encryption key; (c) decrypting the program material using the first encryption key" is shown in '208 col. 7, lines 33-35;

"(d) re-encrypting the program material according to a second encryption key; and" is disclosed in '208 col. 7, lines 34-38;

the following is not explicitly taught in '208: **"(e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; (f) providing the re-encrypted program material and the fourth encryption key for storage"** however '208 teaches "various means to incorporate a means of tracking the number of copies made of the content in col. 3, line 64 through col. 4, line 28; in addition '208 teaches "As shown in FIG. 3, the transfer control data contain four bits ... representing a transfer generation number (a copy generation number) ... Each time transferring or copying contents data is executed, the transfer-source player or apparatus (the copy-source player or apparatus) processes the transferred data or the copied data so that the number represented by the transfer-generation-number data piece is decremented by "1". When the transfer-generation-number data piece reaches "0000", transferring or copying contents data is prohibited. For example, the transfer-source player or apparatus (the copy-source player or apparatus) is disabled by the transfer-generation-number data piece being "0000" in col. 8, line 47 through col. 9, line 3. As well '208 teaches "The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" in col. 7, lines 34-38 it is obvious by the text "other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" that as long as the transfer-generation-number contained in the header is not "000" that a new encryption key will be generated and included in the 'encryption-resultant playback key data'. As well '208 teaches "step S34 subsequent to the step S33 encrypts the primary encryption-resultant playback key data into other secondary encryption-resultant playback key data or third encryption-resultant playback key data in response to the ID of the copy-destination player (the transfer-destination player) 6b. A step S35 following the step S34 transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data (generated by the step S34) to the copy-destination player 6b. The customer's player 6b recovers the original contents data as the customer's player 6a does (see FIG. 9). After the step S35, the current execution cycle of the program segment ends. The customer's player 6a is designed to upload the transfer control data representative of the transfer generation number (the copy generation number) to a host side each time the transfer generation number is updated." in col. 12, lines 25-48, this obviously would mean that each time the transfer generation number, and the encryption-resultant playback key data is updated, another key is generated, i.e. 'fourth encryption key', then fifth, sixth, etcetera.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated by generating a new encryption key. One of ordinary skill in the art would have been motivated to perform such a modification because it is desirable to manage copyright data see '208 (col. 1, lines 39 et seq.) "It is desirable to prevent contents data from being transmitted and downloaded to an illegal customer's player. Even in the case where contents data have been transmitted and downloaded to a legitimate customer's player, it is desirable to manage copying the contents data for copyright".

As to dependent claim 2, "wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of: decrypting the received access control information to produce the temporally variant control data; and modifying the temporally variant control data to generate temporally-invariant control data" is taught in '208 col. 7, lines 13-25.

As to dependent claim 15, "wherein the control data is temporally-variant" is disclosed in '208 col. 7, lines 35-38.

As to independent claim 17, "An apparatus for: storing program material encrypted according to a first encryption key for replay, comprising: a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data" is taught in '208 col. 7, lines 13-25;

"the control access module comprising a first decryption module, for decrypting the access control information to produce the first encryption key" is shown in '208 col. 7, lines 33-35;

the following is not explicitly taught in '208:

"a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and a second decryption module for decrypting the fourth encryption key to produce the second encryption key" however '208 teaches "various means to incorporate a means of tracking the number of copies made of the content in col. 3, line 64 through col. 4, line 28; in addition '208 teaches "As shown in FIG. 3, the transfer control data contain four bits ... representing a transfer generation number (a copy generation number) ... Each time transferring or copying contents data is executed, the transfer-source player or apparatus (the copy-source player or apparatus) processes the transferred data or the copied data so that the number represented by the transfer-generation-number data piece is decremented by "1". When the transfer-generation-number data piece reaches "0000", transferring or copying contents data is prohibited. For example, the transfer-source player or apparatus (the copy-source player or apparatus) is disabled by the transfer-generation-number data piece being "0000" in col. 8, line 47 through col. 9, line 3. As well '208 teaches "The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" in col. 7, lines 34-38 it is obvious by the text "other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" that as long as the transfer-generation-number contained in the header is not "000" that a new encryption key will be generated and included in the 'encryption-resultant playback key data'. As well '208 teaches "step S34 subsequent to the step S33 encrypts the primary encryption-resultant playback key data into other secondary encryption-resultant playback key data or third encryption-resultant playback key data in response to the ID of the copy-destination player (the transfer-destination player) 6b. A step S35 following the step S34 transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data (generated by the step S34) to the copy-destination player 6b. The customer's player 6b recovers the original contents data as the customer's player 6a does (see FIG. 9). After the step S35, the current execution cycle of the program segment ends. The customer's player 6a is designed to upload the transfer control data representative of the transfer generation number (the copy generation number) to a host side each time the transfer generation number is updated." in col. 12, lines 25-48, this obviously would mean that each time the transfer generation number, and the encryption-resultant playback key data is updated, another key is generated, i.e. 'fourth encryption key', then fifth, sixth, etcetera.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated by generating a new encryption key. One of ordinary skill in the art would have been motivated to perform such a modification because it is desirable to manage copyright data see '208 (col. 1, lines 39 et seq.) "It is desirable to prevent contents data from being transmitted and downloaded to an illegal customer's player. Even in the case where contents data have been transmitted and downloaded to a legitimate customer's player, it is desirable to manage copying the contents data for copyright".

As to dependent claim 18, further comprising: a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is shown in '208 col. 6, lines 34-48 (Note tuner is considered equivalent to a communication device that communicates with a satellite);

"a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module; a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key" is disclosed in '208 col. 3, line 64 through col. 4, line 28.

As to dependent claim 25, "wherein the second encryption key is stored in the conditional access module" is taught in '208 col. 7, lines 13-38.

As to dependent claim 26, "wherein the third encryption key is stored in the conditional access module" is shown in '208 col. 7, lines 13-38.

As to dependent claim 27, "wherein the conditional access module is releaseably communicative coupleable to: a tuner for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is taught in '208 col. 6, lines 33-48;

"a third decryption module, for decrypting the program material using the first encryption key from the conditional access module a second encryption module, for re-encrypting the decrypted program material according to the key" is shown in '208 col. 7, lines 13-48;

"and a media storage device" is disclosed in '208 col. 6, lines 49-67.

As to independent claim 28, this claim is directed to the apparatus implementing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 29, 36, 40, and 41, these claims contain substantially similar subject matter as claims 2, 10, 14, and 15; therefore they are rejected along similar rationale.

As to dependent claim 43, "further comprising the step of generating the second encryption key in the conditional access module" is taught in '208 col. 7, lines 13-48.

11. **Claims 4-14, 16, 19-24, 31-35, 37, 38, 39, 42 and 44-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over '208 in view of Atkins, III et al. U.S. Patent No. 6,560,340 (hereinafter '340).

As to dependent claim 4, the following is not taught in '208: "wherein the conditional access module on a smartcard" however '340 teaches "DHCTSE 627 includes a microprocessor (capable of performing DES), specialized hardware for performing RSA encryption and decryption, and secure memory elements. All of the components of DHCTSE 627 are contained in a single tamper-proof package, such as a package that upon attempting to access the information contained within the information is destroyed. Only the components of DHCTSE 627 have access to the information stored in the secure memory elements. Any attempt by a user to gain access to any of the parts of DHCTSE 627 renders DHCTSE 627 unusable and its contents unreadable. DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a "smart card" in col. 21, lines 1-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include an improved means of distributing content data. One of ordinary skill in the art would have been motivated to perform such a modification because more flexible means are needed to distribute data see '340 (col. 2, lines 60 et seq.) "Thus, the service distribution organizations require access restrictions which are both more secure and more flexible than those in conventional systems.

As to dependent claim 5, "wherein the access control information further comprises metadata describing at least one right for the program material" is shown in '340 col. 4, lines 50-61.

As to dependent claim 6, "further comprising the step of generating the second encryption key at least in part from the metadata" is disclosed in '340 col. 4, lines 50-61.

As to dependent claim 7, "wherein steps (b)-(f) are performed in response to a pre-buy Message" is taught in '340 col. 12, lines 39-67.

As to dependent claim 8, "wherein the access control information further comprises metadata describing at least one right for the program material and the method further comprises the step of: generating replay right data from the metadata" is shown in '340 col. 31, lines 7-24.

As to dependent claim 9, "wherein the replay right dam is further generated from pre-buy data" is disclosed in '340 col. 31, lines 7-24.

As to dependent claim 10, "further comprising the steps of retrieving the stored re-encrypted program material and the fourth encryption key; decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and decrypting the re-encrypted material using the second encryption key" is taught in '340 col. 6, lines 24-53.

As to dependent claim 11, "wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material" is shown in '340 col. 30, lines 38-67.

As to dependent claim 12, "wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further comprises the steps of; generating replay right data from the metadata; accepting the buy data; comparing the buy data with the replay right data; and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data" is disclosed in '340 col. 12, line 56 through col. 13, line 39.

As to dependent claim 13, "wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein: the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata sued the pie-buy message in the smartcard; and the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data arid the replay right data tire performed in the smartcard" is taught in '340 col. 21, lines 1-40.

As to dependent claim 14, "wherein the re-encrypted program material and the fourth encryption key ate stored on a media storage device" is shown in '340 col. 7, lines 49-55.

As to dependent claim 16, "wherein the temporally-variant control data associates an expiration time with the program material" is taught in '340 col. 28, line 43 through col. 29, line 39.

As to dependent claim 19, "wherein the conditional access module further comprises: a pre-buy module, for controlling the first decryption module" is taught in '340 col. 12, line 56 through col. 13, line 14.

As to dependent claim 20, "wherein the access control information further comprises metadata describing at least one right for the program material" is shown in '340 col. 31, lines 7-24.

As to dependent claim 21, "wherein pre-buy module generates replay right data from the metadata" is disclosed in '340 col. 12, lines 39-67.

As to dependent claim 22, "further comprising a buy module, communicatively coupled to the pre-buy module" is taught in '340 col. 14, lines 21-67.

As to dependent claim 23, "wherein the buy module comprises: a purchase module; for accepting buy data, and comparing the buy data and the replay right data from the pre-buy module; and a control module for controlling the second decryption module based on the comparison between the buy data and the replay right data" is shown in '340 col. 13, lines 14-54.

As to dependent claim 24, "further comprising a billing module, for recording the buy data" is disclosed in '340 col. 40, lines 2-5.

As to dependent claims 31-35, 37-39, and 42, these claims contain substantially similar subject matter as claims 4-13, and 16; therefore they are rejected along similar rationale.

As to dependent claim 44, "wherein the access control information further comprise metadata and the method further comprises the step of generating the second encryption key at least in part from metadata" is disclosed in is disclosed in '340 col. 4, lines 50-61.

As to dependent claim 45, "further comprising the step of: augementing the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is taught in '340 col. 4, lines 50-61.

As to dependent claim 46, "wherein the access control information further comprises metadata describing at least one right for the program material" is shown in '340 col. 4, lines 50-61;

"and the method further comprises the step of : augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is disclosed in '340 col. 4, lines 50-61.

As to dependent claim 47, "wherein the conditional access module generates the second encryption key at least in part from the metadata" is disclosed in '340 col. 4, lines 50-61.

As to dependent claim 48, "wherein the access control information further comprises a metadata and the conditional access module generated the second encryption key at least in part from the metadata" is disclosed in '340 col. 4, lines 50-61.

As to dependent claim 49, "wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is taught in '208 col. 7, lines 13-25.

As to dependent claim 50, "wherein the access control information further comprises metadata, and wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is disclosed in '340 col. 4, lines 50-61.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT
Ellen Tran
Patent Examiner
Technology Center 2134
7 August 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100